Section:	06	Title:	Information Security
Sub Section:	03	Title:	Information Security
Document:	03	Title:	Password Controls

1. STANDARD

Systems which use passwords on or through ISD systems will conform to ISD Security controls as represented in the procedures listed below.

1.1. Summary of Standard Changes

1.2. Purpose

Standard is used to authenticate a user's identity and to establish accountability.

1.3. Scope

All users of any ISD system for information storage, processing, or communications.

1.4. Responsibilities

Management is responsible to support and maintain all aspects of the standard

1.5. Definitions and Abbreviations

1.6. Description of Standard

The standard forms one of the foundations for the security of the information held by ISD. It establishes required controls for passwords including creation, procedures for use, and basic protection.

1.7. Implications

Users are held accountable for proper password creation and protection. Without these controls user accountability and identity cannot be established. All computers permanently or intermittently connected to ADOA ISD networks must have password access controls. Multi-user systems must employ user Ids and passwords unique to each user. Computer and communication system access control must be achieved by passwords that are unique to each individual user.

1.8. References

1.9. Attachments

2. PASSWORD CREATION PROCEDURES

2.1. Summary of Procedure Changes

2.2. Procedure Details

2.2.1. Passwords are created with and minimum of 6 alpha numeric characters in random order.

2.2.2. Password will not include personal items (names, hobby items, special dates, pet names, etc.).

2.3. References

2.4. Attachments

3. PASSWORD USAGE PROCEDURES

3.1. Summary of Procedure Changes

3.2. Procedure Details

3.2.1. Passwords are not written down or notated in any way in the workplace or any place else where they might be observed by unauthorized persons.

3.2.2. Passwords are changed, at a minimum, every 30 days.

3.2.3. When workstations or monitors are not in use they will be left in a ‘secure screen’ mode with password protection.

3.3. References

3.4. Attachments

4. PASSWORD PROTECTION PROCEDURES

4.1. Summary of Procedure Changes

4.2. Procedure Details

4.2.1. Passwords are never divulged to other employees, including supervisors under any circumstances.

4.2.2. If a password is requested by any person, the circumstance are immediately reported to the ISD Security Manager.

4.2.3. If a password is suspected to have become public it will immediately by changed.

4.2.4. Wherever systems software permits, initial passwords issued to a new user by a security administrator must be valid only for the new user's first session. The confidential user password will then be created by the user during the first session.

4.2.5. System resources accessed by shared passwords ('group passwords') are not permitted.

4.2.6. Password are not stored in readable form in batch files, log-in scripts, software macros, function keys, etc. or any other locations where unauthorized persons might discover them.

4.3. References

4.4. Attachments